UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/803,341	03/18/2004	Kais Belgaied	03226/336001; P8935	5574

32615 7590 07/31/2007

OSHA LIANG L.L.P./SUN
1221 MCKINNEY, SUITE 2800
HOUSTON, TX 77010

EXAMINER	
KIM, JUNG W	
ART UNIT	**PAPER NUMBER**
2132	
MAIL DATE	**DELIVERY MODE**
07/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/803,341	BELGAIED ET AL.	
	Examiner	Art Unit	
	Jung Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-58 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-58 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-58 are pending.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 29-57 are rejected under 35 USC 101 because these claims define a system claim but do not define any hardware elements. The Specification discloses the kernel consumer, cryptographic providers and encryption framework in terms of processes or software modules. See for example, Specification, pg. 5, paragraph 16. Processes or software modules per se are not statutory subject matter.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 2-4, 7, 9-28, 30-33 and 52 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. Claim 2 defines 4 situations but only defines 3 steps for 3 of the situations: 1) if the request is synchronous, performing a cryptographic function in a kernel consumer

context; 2) if the request is asynchronous and the kernel consumer indicated to queue the request, queuing the request; 3) if the request is asynchronous and the kernel consumer indicated not to queue the request, and the request does not need to be queued, performing the cryptographic function and returning the result. However, a fourth step is omitted for the fourth situation, that situation being 4) if the request is asynchronous and the kernel consumer indicated not to queue the request, and the request needs to be queued. It is not clear what step is required in this fourth scenario. This omission renders the claim incomplete.

7. Claim 3 defines 3 situations but only defines 2 steps for 2 of the situations: 1) if queue resources are available then notifying the kernel consumer that the request has been successfully queued; 2) if no queue resources are available and the request is asynchronous then notifying the kernel consumer that the request to queue has failed. However, a third step is omitted for the third situation, that situation being 3) if no queue resources are available and the request is synchronous (not asynchronous). Moreover, claim 3 and its parent claims only define queuing the request if the request is asynchronous and the kernel consumer indicated to queue the request. (Claim 2). Hence, either the limitation "if ... the request is asynchronous" is superfluous, or the claim (or parent claim(s)) must define a step where the request is queued if the request is not asynchronous. The omission renders the claim incomplete.

8. Claim 4 defines 2 situations but only defines 1 step for 1 of the situations: 1) "if the request is asynchronous, registering the kernel ... and resubmitting the request ..." However, a second step is omitted for the second situation, that situation being 2) if the

request is synchronous (not asynchronous). Moreover, claim 4 and its parent claims only define queuing the request if the request is asynchronous and the kernel consumer indicated to queue the request. (Claim 2). Hence, either the limitation "if the request is asynchronous" is superfluous, or the claim (or parent claim(s)) must define a step where the request is queued if the request is not asynchronous. The omission renders the claim incomplete.

9. Claim 7 defines 2 situations but only defines 1 step for 1 of the situations: 1) if the request is asynchronous, the request is performed in an interrupt context. However, a second step is omitted for the second situation, that situation being 2) if the request is synchronous (not asynchronous). It is not clear what step is required in this second scenario. This omission renders the claim incomplete.

10. Claim 9 defines 4 situations but only defines 3 steps for 3 of the situations: 1) if the request is synchronous, performing a cryptographic function in a kernel consumer context; 2) if the request is asynchronous and the kernel consumer indicated to queue the request, queuing the request; 3) if the request is asynchronous and the kernel consumer indicated not to queue the request, and the request does not need to be queued, performing the cryptographic function. However, a fourth step is omitted for the fourth situation, that situation being 4) if the request is asynchronous and the kernel consumer indicated not to queue the request, and the request needs to be queued. It is not clear what step is required in this fourth scenario. This omission renders the claim incomplete.

11. Claims 10-13 do not remedy the omission of parent claim 9.

12. Claim 14 defines 3 situations but only defines 2 steps for 2 of the situations: 1) if queue resources are available then notifying the kernel consumer that the request has been successfully queued; 2) if no queue resources are available and the request is asynchronous then notifying the kernel consumer that the request to queue has failed. However, a third step is omitted for the third situation, that situation being 3) if no queue resources are available and the request is synchronous (not asynchronous). Moreover, claim 14 and its parent claim only define queuing the request if the request is asynchronous and the kernel consumer indicated to queue the request. (Claim 9). Hence, either the limitation "if ... the request is asynchronous" is superfluous, or the claim (or parent claim(s)) must define a step where the request is queued if the request is not asynchronous. The omission renders the claim incomplete.

13. Claim 15 defines 2 situations but only defines 1 step for 1 of the situations: 1) "if the request is asynchronous, registering the kernel ... and resubmitting the request ..." However, a second step is omitted for the second situation, that situation being 2) if the request is synchronous (not asynchronous). Moreover, claim 4 and its parent claims only define queuing the request if the request is asynchronous and the kernel consumer indicated to queue the request. (Claim 2). Hence, either the limitation "if the request is asynchronous" is superfluous, or the claim (or parent claim(s)) must define a step where the request is queued if the request is not asynchronous. The omission renders the claim incomplete.

14. Claims 16-28 do not remedy the omission of parent claim 9.

15. Claim 30 defines 2 situations but only defines 1 step for 1 of the situations: 1) if the request is synchronous, perform the cryptographic function in a kernel consumer context. However, a second step is omitted for the second situation, that situation being 2) if the request is asynchronous (not synchronous). It is not clear what step is required in this second scenario. The omission renders the claim incomplete.

16. Claim 31 defines 2 situations but only defines 1 step for 1 of the situations: 1) if the request is asynchronous and the kernel consumer indicated that the request is to be queued, queue the request. However, a second step is omitted for the second situation, that situation being 2) if the request is synchronous (not asynchronous) or the kernel consumer did not indicate that the request is to be queued. It is not clear what step is required in this second scenario. The omission renders the claim incomplete.

17. Claim 32 defines 2 situations but only defines 1 step for 1 of the situations: 1) if the request is queued, return a handle to the kernel consumer. However, a second step is omitted for the second situation, that situation being 2) if the request is not queued. It is not clear what step is required in this second scenario. The omission renders the claim incomplete.

18. Claim 33 does not remedy the omission of parent claims 31 and 32.

19. Claim 52 recites the limitation "the context template". There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

20. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

21. Claims 1, 5, 6, 8 and 29-58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leung et al. USPN 7,120,799 (hereinafter Leung) in view of Ueno et al. USPN 5,301,331 (hereinafter Ueno).

22. As per claims 1, 5, 6 and 8, Leung discloses a method for performing a cryptographic function comprising:

a. Calling into an encryption framework to perform the cryptographic function, wherein calling into the encryption framework comprises sending a request to perform the cryptographic function from a kernel consumer; processing the request and returning the result to the kernel consumer wherein processing the request comprises determining whether the request is to be performed by a hardware process or a software process, and determining which cryptographic provider to use to perform the cryptographic function; wherein the cryptographic provider comprises at least one selected from the group consisting of a hardware provider and a software provider; (fig. 3; col. 5:48-55)

b. Wherein the hardware provider is associated with a hardware provider queue and the software provider is associated with a software provider queue; (5:64-6:4)

c. Wherein the encryption framework is located in a kernel and comprises a kernel interface configured to interface between the encryption framework and the kernel consumer, and a provider interface configured to interface between the cryptographic provider and the kernel interface. (fig. 3, reference nos. 312, 304 and 306)

23. Leung does not expressly disclose wherein processing the request comprises determining whether the request is synchronous or asynchronous. Ueno discloses a method and system for facilitating execution of a user-input message whereby a queuing unit is used to determine whether an instruction received is a synchronous type or an asynchronous type; if the instruction is a synchronous type, the instruction is executed and the results forwarded back to the user, otherwise if the instruction is an asynchronous type, the instruction is queued, and an identifier is generated to match the instruction to be executed in the future (Abstract; col. 4:44-5:27; fig. 7: "Asynchronous process queue") Such executing means enables improvement in CPU performance. (1:36-47) Moreover, Leung discloses that in software implementation, no additional I/O connections are necessary once the code is loaded into memory, whereas hardware requires additional connections to the operating machine. (2:8-17) This discussion points to a conventional knowledge in the art that hardware providers typically operate in asynchronous mode due to the fact that hardware requires multiple I/O operations and any downtime while the hardware waits for the I/O operation to complete would substantially slow down the performance. Software typically operates in either asynchronous or synchronous mode; software is not restricted to one mode

because it is loaded into memory and does not suffer the delays caused by I/O operation completion. (See also applicant's Specification, paragraphs 24 and 25) Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made wherein processing the request comprises determining whether the request is synchronous or asynchronous. One would be motivated to do so as asynchronous processing for hardware providers enables processing to continue while waiting for I/O operations to complete, whereas synchronous processing for software providers employ a simpler means of execution and do not experience the delay waiting for I/O operations to complete as known to one of ordinary skill in the art. The aforementioned cover the limitations of claims 1, 5, 6 and 8.

24. As per claims 29-45, Leung discloses a system for performing a cryptographic function, comprising:

d. a kernel consumer configured to request the cryptographic function (fig. 3), and a kernel comprising:

i. a cryptographic provider configured to perform the cryptographic function (fig. 3, reference nos. 308 and 310), and

ii. an encryption framework comprising:

(1) A kernel interface configured to interface between the encryption framework and the kernel consumer, (fig. 3, reference nos. 312 and 306) and

(2) A provider interface configured to interface between the cryptographic provider and the kernel interface (fig. 3, reference nos. 304 and 306),

iii. Wherein the encryption framework is configured to receive and schedule requests to be performed by a hardware process or a software process; (5:48-55)

iv. Wherein the encryption framework is configured to notify the kernel consumer if queue resources are not available or when queue resources are available; (5:64-67)

v. Wherein the cryptographic provider comprises at least one selected from the group consisting of a hardware provider and a software provider; (abstract; 5:48-55)

vi. Wherein a hardware provider queue is associated with the hardware provider; and a software provider queue is associated with the software provider; (5:64-6:4)

vii. Wherein the kernel interface is configured to notify the kernel consumer when the cryptographic provider has completed performing the cryptographic function; (fig. 4, step 412)

viii. Wherein the encryption framework is configured to generate a context template, wherein the context template is associated with the request; wherein the encryption framework is configured to initialize and compute portions of the context template; (6:63-7:8)

ix. wherein the request comprises a cryptographic mechanism; wherein the framework further comprises a list of cryptographic mechanisms provided by the cryptographic provider; wherein the encryption framework is configured to load the cryptographic provider into the kernel using the list of cryptographic mechanisms and a cryptographic mechanism in the request; (6:50-62; 7:45-65)

x. wherein the encryption framework comprises functionality to dynamically add or remove a mechanism. (6:5-10)

25. Leung does not expressly disclose wherein processing the request comprises determining whether the request is synchronous or asynchronous; wherein the encryption framework is configured to perform the cryptographic function in a kernel consumer context if the request is synchronous; wherein the encryption framework is configured to queue the request if the request is asynchronous and the kernel consumer indicated that the request is to be queued; wherein the encryption framework is configured to return a handle to the kernel consumer if the request is queued; wherein the kernel consumer may cancel the request using the handle.

26. Ueno discloses a method and system for facilitating execution of a user-inputted message whereby a queuing unit is used to determine whether an instruction received is a synchronous type or an asynchronous type; if the instruction is a synchronous type, the instruction is executed and the results forwarded back to the user, otherwise if the instruction is an asynchronous type, the instruction is queued, and an identifier is generated to match the instruction to be executed in the future (Abstract; col. 4:44-5:27;

fig. 7: "Asynchronous process queue"). The asynchronous CPU resource using process produces an interruption factor that can initiate an interrupt, which can terminate any queued processes before being processed under exceptional circumstances (Abstract, 5:28-7:45). Such executing means enables improvement in CPU performance. (1:36-47) Moreover, Leung discloses that in software implementation, no additional I/O connections are necessary once the code is loaded into memory, whereas hardware requires additional connections to the operating machine. (2:8-17) This discussion points to a conventional knowledge in the art that hardware providers typically operate in asynchronous mode due to the fact that hardware requires multiple I/O operations and any downtime while the hardware waits for the I/O operation to complete would substantially slow down the performance of the hardware. Software typically operates in either asynchronous or synchronous mode; software is not restricted to one mode because it is loaded into memory and does not suffer the delays caused by I/O operation completion. (See also applicant's Specification, paragraphs 24 and 25) Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made wherein processing the request comprises determining whether the request is synchronous or asynchronous; wherein the encryption framework is configured to perform the cryptographic function in a kernel consumer context if the request is synchronous; wherein the encryption framework is configured to queue the request if the request is asynchronous and the kernel consumer indicated that the request is to be queued; wherein the encryption framework is configured to return a handle to the kernel consumer if the request is queued; wherein

the kernel consumer may cancel the request using the handle. One would be motivated to do so as asynchronous processing for hardware providers enables processing to continue while waiting for I/O operations to complete, whereas synchronous processing for software providers employ a simpler means of execution and do not experience the delay waiting for I/O operations to complete as known to one of ordinary skill in the art. The aforementioned cover the limitations of claims 29-45.

27. As per claims 46-57, the rejections of claims 29-45 under 35 USC 103(a) as being unpatentable over Leung in view of Ueno are incorporated herein. In addition, Leung discloses wherein the kernel interface is configured to notify the kernel consumer when one of the plurality of cryptographic providers has completed performing the cryptographic function. (fig. 4, step 412) The aforementioned cover the limitations of claims 46-57.

28. As per claim 58, the rejections of claims 46-57 under 35 USC 103(a) as being unpatentable over Leung in view of Ueno are incorporated herein. In addition, Leung does not disclose wherein the kernel consumer executes on any node of the plurality of nodes, wherein the cryptographic provider executes on any node of the plurality of nodes, wherein the provider interface executes on any of the plurality of nodes, and wherein the kernel interface executes on any node of the plurality of nodes. However, it has been found that arrangement and reversible of parts is an obvious enhancement. See In re Gazda, 219 F.2d 449 and In re Japikse, 181 F.2d 1019. Further, it is

notoriously well known in the art that the functionality of computing nodes are generally interchangeable due to the "black box" nature of a computing processor. Examiner takes Official notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Leung such that wherein the kernel consumer executes on any node of the plurality of nodes, wherein the cryptographic provider executes on any node of the plurality of nodes, wherein the provider interface executes on any of the plurality of nodes, and wherein the kernel interface executes on any node of the plurality of nodes. One would be motivated to do so to provide flexibility in arranging the system as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 58.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132